Software-Defined Mobility

Foundational technology for the fully mobile enterprise

Enterprises across every sector are racing to embrace mobile technologies for their workforces. Among IT decision makers, 87 percent report that enterprise mobility is critical to their company's profitability, and nearly three-fourths say their companies are planning to mobilize their entire organization. IDC projects that mobile workers will account for 72 percent of the U.S. workforce by 2020.

Enterprises expect that workers will be able to access enterprise applications from everywhere. Among technology decision makers in North America, 61% are implementing mobile productivity apps, 55% file sync and share apps, and 55% collaboration apps.

However, reliable application delivery in mobile environments is far-more challenging to IT than in the wired world. The mobile enterprise depends on networks that are under others' administrative control. Over those networks, there will be more mobile apps dedicated to business use, vying for bandwidth on increasingly congested infrastructure. More than a half a billion new mobile devices and connections were added in 2015 alone, and mobile data use is projected to increase eightfold over the next five years.

The Building Blocks

A Software-Defined Mobility architecture provides a flexible way to stitch together disparate networks that are both inside and outside of the administrative control of enterprises. Creating a single virtual network with a common point of control provides a solution for reliable application delivery over disparate, unpredictable networks. Fundamentally, the architecture is straightforward: a lightweight software client on each mobile device, and a server in the cloud or data center that sits in front of the enterprise applications. A controller that is co-resident with the server handles the configurations and pushes out policy rules and associated actions for execution by the client. The policies are evaluated as the device runs applications, accesses different networks and moves between them, and encounters variable network conditions.

The control functions are visualized and maintained at the server, but control execution and traffic forwarding happen at the client. This offers a programmatic way to customize and virtualize underlying networks regardless of performance and location, so that IT can optimize, secure, manage and administer their workers' connections for maximum application availability, reliability and performance.

Software-Defined Networking and the Challenges of Mobility

In a wired network, a Software-Defined Network (SDN) enables the programming of Ethernet routers and switches to define the behavior of the network. The forwarding of traffic is separated from control over how the traffic is forwarded. This decoupling allows administrators to control multiple devices from a software-based SDN controller that provides a global view of the network, dynamically adjust network-wide traffic flow to meet changing needs, and use automated programs to configure, manage, secure and optimize network resources very quickly.

When the principles of Software-Defined Networking are applied to mobile networks, the proposed designs rely on federated or shared administrative domains across cellular and Wi-Fi networks. These designs are impractical for modern, fully mobile enterprises. That is because mobile workers use a mix of cellular and Wi-Fi connections that include residential, carrier, privately owned and enterprise networks to establish connectivity for their applications — an extremely heterogenous combination outside the scope of what can be realistically federated.

Instead of physically separating control from traffic forwarding, Software-Defined Mobility separates them logically and puts IT control of the endpoints. Administrators can control application delivery based on changing network conditions through software, regardless of the combination of networks used.

As employees move from one network condition to another, the system adapts by using match criteria and preprogrammed actions to virtualize the underlying networks. The policies are managed centrally and pushed out over the air. The Software-Defined Mobility architecture provides an abstraction layer for applications and flows to increase reliability and performance. Applications are shielded from the effects of roaming, varying security requirements and unpredictable networks.

Software-Defined Mobility: A Unique Set of Advantages

Applying Software-Defined Mobility gives IT an unprecedented degree of control over the performance, reliability and security of the mobile environment.

Traffic Optimization enables workers to roam seamlessly among any combination of networks, device connections continue through coverage gaps, and optimization allow applications to run reliably over weak and intermittent network conditions.

Adaptive Policies prioritize application access based on network and situation/location parameters. Policies can prevent access to bandwidth-intensive applications over slow networks which reduces mobile device functionality. Policies are network-aware and can push data-demanding maintenance, updates and upgrades to unmetered Wi-Fi or wired networks when they are accessible.

Performance Analytics and Diagnostics deliver real-time big data on connections, network use and conditions, bandwidth consumption, application access and device locations. For mobile environments, this includes public networks that are outside the firewall, and the variety of mobile devices (BYOD, COPE, etc.) and platforms being deployed. With this information IT can control costs, fine-tune policies and improve the user experience and productivity. Having the analytics and visualization tools available, decision makers are equipped with the key intelligence for improving business operations that can now extend beyond the firewall. Furthermore, when problems are detected, NetMotion's diagnostic capabilities can launch automatically to determine the root cause of failures or underperformance.

Security through Software-Defined Mobility supports a highly flexible and programmable VPN. It offers split tunneling on a per-app, per-flow basis, or device-wide locking down the device requiring all traffic to route through the secure enterprise network. It includes integration with multi-factor authentication systems, SIEM tools, and alerting. Quarantine lost or stolen devices to prevent access to corporate resources. With the addition of NetMotion's diagnostic tools, WiFi security issues can also be tracked and alleviated.

Essential Capability for Enterprise Mobility

As more enterprises go mobile, they will face the challenges of reliably delivering applications over the variable conditions encountered in mobile networks. Only Software-Defined Mobility — an approach used in thousands of mobile deployments worldwide — has been proven to deliver the same reliable performance, control and security that IT currently is able to exert over their wired networks.

Selected references

EnterpriseMobilitySurvey_Appian.htm

EnterpriseMobilitySurvey_Appian.htm

EnterpriseMobilityExplosiveGrowth_ProKarma.htm

2015-07-17-VMWare-Mobility-Insights-from-Technology-and-Business-Decision-Makers.pdf

Cisco Visual Networking Index:
Global Mobile Data Traffic Forecast Update, 2015–2020

Software Defined Networking Definition.
https://www.opennetworking.org/sdn-resources/sdn-definition